

12-15-99

A

Y. Hsu 1

"Express Mail" mailing label number EJ466720715US, Date of Deposit 12/14/1999  
I hereby certify that this Application is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231.

Thomas Stafford  
Printed Name of Mailing Person

Thomas Stafford  
Signature of Mailing Person

**IN THE UNITED STATES  
PATENT AND TRADEMARK OFFICE**

**PATENT APPLICATION**

**INVENTOR(s)** Yung-Kao Hsu

**CASE:** 1

**TITLE:** DUAL-TIER SECURITY ARCHITECTURE FOR INTER-DOMAIN  
ENVIRONMENTS

**ASSISTANT COMMISSIONER FOR PATENTS**  
WASHINGTON, D.C. 20231

**SIR:**

Enclosed are the following papers relating to the above-named application for patent:

- 31 Page specification and claims
- 5 Sheets of Informal drawings
- Declaration and Power of Attorney
- Assignment and Agreement
- PTO-1619A and B
- Information Disclosure Statement
- Document

12/14/99



JC690 U.S. PTO  
09/460897



12/14/99

Y. Hsu 1

**CLAIMS AS FILED**

	No. Filed	No. Extra	Rate	Calculations
Total Claims	59-20 =	39	x \$18 =	702
Independent Claims	3 - 3 =	0	x \$78 =	0
Multiple Dependent Claim(s), if applicable	0		\$270 =	0
Basic Fee				760
			TOTAL FEE	<b>1462</b>

Please file the application and charge **Lucent Technologies Deposit Account No. 12-2325** the above-indicated amount, to cover the filing fee. Duplicate copies of this letter are enclosed. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit Deposit Account No.12-2325 as required to correct the error.

Please address all correspondence to **Thomas Stafford, 4173 Rotherham Court, Palm Harbor, Florida 34685**. Telephone calls should be made to Thomas Stafford at 727-772-4173, FAX 727-772-2545.

Respectfully,  
Yung-Kao Hsu

By   
THOMAS STAFFORD  
Attorney for Applicant  
Reg. No. 24767  
727-772-4173

Date: 12/14/1999

## **DUAL-TIER SECURITY ARCHITECTURE FOR INTER-DOMAIN ENVIRONMENTS**

### **Related Application**

This application claims the priority of the corresponding provisional application,  
5 Serial No. 60/129496, filed April 15, 1999.

### **Technical Field**

This invention relates to securing multimedia communication in a data network and, more particularly, in inter-domain environments.

### **Background of the Invention**

10 Most security arrangements rely heavily on the use public-key cryptography, X.509 certificates and public-key infrastructure (PKI) to provide scalability. Critical to such security arrangements is that each end user and user device can be authenticated by an X.509 certificate. However, this assumption may not be viable for future systems because there are serious key management issues relating to PKI design and deployment.  
15 Indeed, there is no real cost effective solution for certificate revocation and key management. Secret-key cryptography, where communicating parties must share a security key in advance, e.g., ID/Password, will continue to play an important role for user authentication in an enterprise or public communication environment. Although secret-key arrangements are simple and highly portable, they are not scalable.

### **Summary of the Invention**

20 Problems and limitations with prior known security arrangements are overcome by employing a two-tier security architecture that provides balance between the use of public and secret-key cryptography to realize cost-effectiveness and scalability of security. One tier is an intra-zone tier and the other tier is an inter-zone tier. The intra-  
25 zone tier addresses communication between users employing endpoints within a prescribed Security Zone and is designed to achieve cost-effectiveness. The inter-zone tier specifies how communication between users employing endpoints from different Security Zones can be established and is designed to provide scalability for intra-enterprise and/or inter-enterprise communications.

30 Specifically, each Security Zone has a "Zone Keeper" and one or more endpoints that may be employed by users. The Zone Keeper authenticates, i.e., validates, users

employing an endpoint in the Security Zone and determines whether a caller and a callee are security compatible. When setting up a communication, the caller provides the Zone Keeper security information in order for the caller to prove its identity. The callee supplies the caller information confirming its identity. A proposal on how the communication is to be Set-up is sent from the caller to the callee, and if they agree to the proposal and their security is authenticated, the communication is started.

For inter-zone, i.e., inter-domain, communications, the caller provides information as described above to its Zone Keeper. Then, the caller's Zone Keeper forwards the caller's request to the Zone Keeper of the Security Zone associated with the callee. Additionally, the caller's Zone Keeper also supplies the callee's Zone Keeper with its security identity so that the callee's Zone Keeper may authenticate that the request is from the caller's Zone Keeper. Then, the callee's Zone Keeper sends back an authorization to the Caller's Zone Keeper. This authorization includes the callee's Zone Keeper security identity so that the caller's Zone Keeper can authenticate that the authorization is from the callee's Zone Keeper. Then, as indicated above, the callee supplies to the caller information confirming its identity. A proposal on how the secure communication is to be Set-up is sent from the caller to the callee and if they agree to the proposal, and their security is authenticated, the communication is started.

In a specific example, the secure communication is directed toward a multimedia application or some other multimedia communication.

One technical advantage of the invention is that individual users/endpoints do not have to know the security mechanism for establishing an inter-zone secure communication. Another technical advantage of the invention is that users/endpoints in different security zones can communicate securely as though they were in the same security zone.

#### **Brief Description of the Drawing**

FIG. 1 shows, in simplified form, details of a two tiered security system including an embodiment of the invention;

FIG. 2 is an information flow diagram illustrating the Set-up process for a secure intra-zone communication between a caller and a callee employing the invention;

FIG. 3 is an information flow diagram illustrating the Set-up process for a secure inter-zone communication between a caller and a callee employing the invention;

FIG. 4 is an information flow diagram illustrating the Set-up process for a H.323 security system secure intra-zone communication between a calling endpoint and a called endpoint employing the invention;

FIG. 5 is an information flow diagram illustrating the Set-up process for a H.323 security system secure inter-zone communication between a calling endpoint and a called endpoint employing the invention;

FIG. 6 is a diagram illustrating the use of security tokens for intra-zone communication between a caller and a callee employing the invention; and

FIG. 7 is a diagram illustrating the use of security tokens for inter-zone communication between a caller and a callee employing the invention.

### **Detailed Description**

FIG. 1 shows, in simplified form, details of a two tiered security system including an embodiment of the invention. Specifically, shown is a multiple zone, i.e., domain, system including Security Zone 101-1 and Security Zone 101-2. For simplicity and clarity of exposition only two Security Zones are shown and described here, however, it will be apparent that any desired number of Security Zones may be employed depending on their manageability. Each of Security Zones 101-1 and 101-2 is a collection of so-called endpoints that are managed as an enterprise. Endpoint devices are intended to operate on behalf of their users to communicate with each other and their so-called Zone Keeper. A Security Zone may be established in any number of environments, for example, a corporate office and/or branch office, a cable system within a prescribed geographical area, a local calling area of a telephone company or the like. Note that physical environments or communication devices do not restrict a Security Zone. For example, a group of users can form a Security Zone if they agree to have their communications be managed by the same Zone Keeper. Thus, Zone Keepers 102-1 and 102-2 are associated on a one-to-one basis with Security Zones 101-1 and 101-2, respectively. A Zone Keeper is an operation, administration, and maintenance facility provided by the enterprise associated with the Security Zone to enforce a security policy for communication in its associated Security Zone and, also, between Zone Keepers

associated with other Security Zones. A Zone Keeper may be a standalone system or a subsystem in, for example, a router, PBX (private branch exchange) or the like. In this example, Security Zone 101-1 includes endpoints 103-1-1, 103-1-2 and 103-1-3, while Security Zone 101-2 includes endpoints 103-2-1, 103-2-2 and 103-2-3. Again, each Security Zone 101 may include as many endpoints 103, as desired only being limited by management issues. Each endpoint is, for example, a data communication device such as a telephone, personal computer, PDA (personal digital assistant), or the like. Communication between Zone Keeper 102-1 and Zone Keeper 102-2, in accordance with a prescribed protocol, is illustrated by communication path 104, as will be described below. Similarly, in this example, communication between endpoint 103-1-2 in Security Zone 101-1 with endpoint 103-2-3 in Security Zone 101-2 is illustrated by communication path 105, in accordance with a prescribed protocol, as will be described below. In this example, communication within Security Zone 101-1, between endpoint 103-1 and Zone Keeper 102-1 is illustrated by communication path 107, in accordance with a prescribed protocol. Communication between endpoint 103-1-1 and endpoint 103-1-2 is illustrated by communication path 106 and communication by endpoint 103-1-2 Zone Keeper 102-1 is illustrated by communication path 108. In Security Zone 101-2, communication between endpoint 103-2-1 and Zone Keeper 102-1 is illustrated by communication path 110. While communication between endpoints 103-2-1 and 103-2-2 is illustrated by communication path 109, and communication between endpoint 103-2-3 and Zone Keeper 102-2 is illustrated by communication path 111, it should be noted that the communications paths simply indicate that data is exchanged between endpoints and/or endpoints and a Zone Keeper and/or Zone Keepers, and the communications paths are not permanent connections.

Note that a Security Zone, has the following characteristics:

- It must have a Zone Keeper (Gatekeeper).
- All calls originated within the Security Zone are routed through the Zone Keeper.
- The Zone Keeper assures the authenticity of every endpoint in the Security Zone.

A Security Zone should be deployed in a secured environment that is not subject to active attacks such as denial-of-service attacks. Examples of such environments are intranets with trusted firewalls, and VPNs (Virtual Private Networks).

It is also felt best to define some terms as follows:

5    **Authentication**        The process of verifying that the respondents are, in fact, who they say they are.

**Digital Signature**    Systems that allow individuals and/or organizations to electronically certify such features as their identity, their ability to pay, or the authenticity of an electronic document.

10   **Integrity**            the property that exchanged data has not been altered in an unauthorized manner.

**Encryption**           a mode of communication in which only the explicitly enabled parties can interpret the communication.

15   **Key management**    the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

**Private-key**           The secret key of a public-private-key cryptography system. This private-key is used to “sign” outgoing messages, and is used to decrypt incoming messages.

20   **Public-Key**            The public-key of a public-private-key cryptography system. This public-key is used to confirm “signatures” on incoming messages or to encrypt a file or message so that only the holder of the private-key can decrypt the file or message.

**Public-Key**

25   **Cryptography**        A cryptography system that uses two different keys to “lock” and “unlock”, i.e., encrypt and decrypt, respectively, messages and files. The two keys are mathematically linked together. An individual’s public-key is distributed to other users and is used to encrypt messages to the individual. The individual keeps the private-key secret and uses it to decrypt messages sent with the public-key. RSA (Rivest, Shamir and Adleman algorithm) and

30

ElGamal are just two examples of public-key cryptography systems.

FIG. 2 is an information flow diagram illustrating the Set-up process for a secure intra-zone communication between a caller 201 and a callee 202 employing the invention. Thus, shown in Security Zone 101-1 are caller 201 employing, for example, endpoint 103-1-1, callee 202 employing, for example, endpoint 103-1-2 and Zone Keeper 102-1. As indicated above, communication between endpoint 103-1-1 and Zone Keeper 102-1 is illustrated by communication path 107 and communication between endpoint 103-1-1 and endpoint 103-1-2 is illustrated by communication path 106. Then, the steps taken in setting up a secure multimedia communication between caller 201 employing endpoint 103-1-1 and callee 202 employing endpoint 103-1-2 are as follows:

- Step 203      Caller 201 sends its request via endpoint 103-1-1 to its Zone Keeper 102-1. The request includes security information so that the identity of caller 201 can be verified.
- Step 204      Zone Keeper 102-1 authenticates, i.e., authenticates the identity of caller 201 and, then, authorizes the request. Zone Keeper 102-1 can determine whether caller 201 and callee 202 are security compatible for their communication. For example, callee 202 may have indicated that it will not accept any communication from caller 202. Also, the endpoint employed by callee 202 may not be able to handle the level of encryption requested by the caller for their communication.
- Step 205      Zone Keeper 102-1 sends its authorization of the request to caller 201. The authorization includes security information for the caller to prove it is indeed Zone Keeper 102-1. Also included in the authorization is the security information for the caller to authenticate callee 202.
- Step 206      Caller 201, employing endpoint 103-1-1, authenticates, i.e., authenticates, the authorization sent by its Zone Keeper 102-1.



- 5           Step 207       Caller 201 requests connection to callee 202. The request includes the authorization from Zone Keeper 102-1 and the security information needed by callee 202 to prove its identity. Also included in the request is a proposal of how the caller – callee communication should be Set-up.
- Step 208       Callee 202, employing endpoint 103-1-2, authenticates, i.e., authenticates the authorization and communication proposal.
- Step 209       Callee 202 sends to caller 201 the agreement for their communication indicating that it accepts the proposal. The agreement includes information proving the identity of callee 202.
- 10           Step 210       Caller 201 authenticates the identity of callee 202.
- Step 211       Based on their agreement the caller 201 and callee 202 start their communication.

          In one example, the above process is employed to establish a secure multimedia application or other secure multimedia communication.

15

          Note that in the above process, Zone Keeper 102-1 is able to authenticate users employing endpoints 103-1-1 through 103-1-3 in Security Zone 101-1 in order to secure communications. The architecture does not mandate the security technology used by Zone Keeper 102-1 to authenticate the identity of each user. It is left to the particular enterprise to select the security technology that it will use based on its own security policy. For example, an enterprise can use an identification and corresponding password (ID/Password) arrangement for performing the authentication, even if it has relative low-level security requirements for the Security Zone. Whatever the enterprise may use as its security arrangement, Zone Keeper 102-1 is able to use the chosen arrangement to authenticate the identity of the requesting user.

20

25

          As an administration facility, Zone Keeper 102-1 provides the capability to register authentication keys and methods for every user employing one of endpoints 103-1 in Security Zone 101-1. To provide additional security, the registration of authentication keys and methods capability may be extended to endpoints 103-1 in Security Zone 101-1. In such an instance, Zone Keeper 102-1 may only honor requests from authenticated users initiated from authenticated endpoints.

30

As an enhancement, users can register with Zone Keeper 102-1 to enforce individual security policies. For example, managers may request that encryption is required for communications among managers. Note that this embodiment of the invention does not require the support of such a registration capability.

5        Zone Keeper 102-1 uses public-key cryptography and digital signature technology to authenticate itself to users employing endpoints 103-1 in zone 101-1. For each response it sends to a user employing an endpoint 103-1, Zone Keeper 102-1 includes a digital signature. Zone Keeper 102-1 creates this signature by “signing” the response message with its private-key. After receiving the response message, an endpoint 103-1  
10 authenticates its signature using the public-key of Zone Keeper 102-1. The architecture of this embodiment of the invention does not specify how the public-key of Zone Keeper 102-1 is distributed to endpoints 103-1. Additionally, the existence of a public-key infrastructure (PKI) is not required in practicing this embodiment of the invention.

It is noted that although the above discussion of intra-zone security used Security  
15 Zone 102-1, Zone Keeper 102-1 and endpoints 103-1, as an example, the processes and techniques discussed are equally applicable to any additional Security Zones including a Zone Keeper and endpoints. Another example being Security Zone 101-2, Zone Keeper 102-2 and endpoints 103-2.

FIG. 3 is an information flow diagram illustrating the Set-up process for a  
20 secure inter-zone communication between caller 301 and callee 302 employing the invention. Shown, is caller 301 employing, for example, endpoint 103-1-2 in Security Zone 101-1, Zone Keeper 102-1 for Security Zone 101-1, Zone Keeper 102-2 for Security Zone 101-2 and callee 302 employing, for example, endpoint 103-2-3 in Security Zone 101-2. Then, the steps taken in setting up a secure multimedia  
25 communication between caller 201 employing endpoint 103-1-1 in Security Zone 101-1, and callee 202 employing endpoint 103-1-2 in Security Zone 101-2 are as follows:

- Step 303        Caller 301, employing endpoint 103-1-2, sends a communication request to Security Zone 101-1 Zone Keeper 102-1.
- Step 304        Zone Keeper 102-1 authenticates the identity of caller 301.
- 30        Step 305        On behalf of caller 301, Zone Keeper 102-1 for Security Zone 101-1 requests authorization, in this example, from Zone Keeper 102-2

for Security Zone 101-2. Realizing that callee 302 is in another Security Zone, Zone Keeper 102-1 forwards the request from caller 301 to Zone Keeper 102-2 for callee 302. However, Zone Keeper 102-1 "signs" the request message with its own private-key so that Zone Keeper 102-2 can authenticate that the request is from Zone Keeper 102-1.

5

Step 306 Zone Keeper 102-2 authenticates the signature of Zone Keeper 102-1 and authorizes the request. Since the request still contains the requirements of caller 301, Zone Keeper 102-1 can determine whether caller 301 and callee 302 are security compatible for the requested communication.

10

Step 307 Zone Keeper 102-2 sends authorization to Zone Keeper 102-1. The authorization includes the digital signature of Zone Keeper 102-2 so that Zone Keeper 102-1 can authenticate that the authorization is indeed from Zone Keeper 102-2. Also included in the authorization is the security information for caller 301 to authenticate callee 302.

15

Step 308 Zone Keeper 102-1 authenticates the authorization sent by Zone Keeper 102-2.

20

Step 309 Zone Keeper 102-1 relays the authorization back to caller 301. Zone keeper 102-1 also attaches its own digital signature to the authorization.

Step 310 Caller 301 authenticates the authorization by verifying the digital signature of Zone Keeper 102-1.

25

Step 311 Caller 301 requests connection to callee 302. The request includes the authorization from Zone Keeper 102-2 and a communication proposal.

Step 312 Callee 302 authenticates the authorization and communication proposal. Callee 302 can verify the digital signature of Zone Keeper 102-2 by using its public-key.

30

Step 313 Callee 302 sends back to caller 301 the agreement for their communication.

Step 314 Caller 301 authenticates the identity of callee 302.

Step 315 Based on their agreements, caller 301 and callee 302 start their communication.

5

Note that the steps taken to establish an inter-zone communication are symmetrical to the steps taken to establish an intra-zone communication. In this particular embodiment, users/endpoints do not have to know the security mechanism for establishing an inter-zone secure communication. Additionally, users/endpoints in different security zones can communicate securely as though they are in the same zone.

10

The inter-zone embodiment requires the Zone Keepers to authenticate each other using public-key cryptography. This requirement allows this embodiment to scale up from intra-zone security.

Additionally, the Zone Keepers each provide the capability to expand its trust to other zones. Specifically, each of the Zone Keepers is able to:

15

1. control a list of trusted zones (A profile may be created for each zone that contains the address of its Zone Keeper and public-key, and security requirements or classifications.);
2. relay the authorization back to the caller and callee endpoints.

## 20 **Implementation of an Embodiment of the Invention in H.323**

H.323 is an ITU-T standard defined for multimedia communication.

The protocols and their security required in this embodiment are summarized as follows:

25

- RAS - RAS (Registration, Admission and Status) provides the vehicle for the Gatekeeper (Zone Keeper) to manage endpoints and their requests within a H.323 zone. Endpoint authentication, integrity of RAS packets, and access control are the primary security issues. RAS uses UDP (User Datagram Protocol) as the transport mechanism.
- Q.931 - This protocol uses TCP (Transport Control Protocol) as its transport mechanism. Its role is to originate the first of many possible point-to-point communications between two endpoints. This Q.931 protocol needs to be secured because it is used to exchange authorization and subsequent security

30

information between endpoints. The security issues for Q.931 are message authentication, encryption, and integrity.

- H.245 - This protocol uses TCP as its transport mechanism. It carries control messages governing endpoint operations, including capabilities exchange and media stream privacy. The security of a H.235 connection is first negotiated by Q.931 messages. It has the same security requirements as Q.931.
- RTP/RTCP (Real time Protocol/Real Time Control Protocol) - This is a Media Stream protocol suite that governs the transportation of video and audio packets. The primary security issue for the Media Stream is encryption.

The security of RAS messaging is most critical for the architecture. Both authentication and authorization information obtained by RAS message exchanges provide the basis for implementing Q.931, H.245, and Media Stream security.

It is felt best to discuss certain H.323 terminology prior to pursuing further disclosure of this embodiment of the invention on H.323.

- Gatekeeper ( hereinafter Zone Keeper) a H.323 entity on the network that provides address translation and controls access to the network for H.323 endpoints. Note Zone Keeper (Gatekeeper) is an optional component in H.323 but is required in the embodiment of the invention.
- H.323 Endpoint - a H.323 terminal, Gateway, or MCU. An endpoint can call and be called. It generates and/or terminates information streams.
- H.323 entity - any H.323 component, including terminal, Gateway, Gatekeeper, MC (Multipoint Controller), MP (Multipoint Processor), and MCU (Multipoint Control Unit).

FIG. 4 is an information flow diagram illustrating the call setup process between a calling endpoint and a called endpoint in H.323.

Step 401      Endpoint (EP1) 103-1-1 in Zone 101-1 sends an ARQ (Admission Request) message to Zone Keeper (ZK1) 102-1.

Step 402      ZK1 sends an ACF (Admission Confirmed) message if the request is accepted or an ARJ (Admission Rejected) message back to EP1.

The ACF message includes the Q.931 port number of endpoint (EP2) 103-1-2.

- Step 403 EP1 then sends a Set-up message to EP2 including the port number of EP2.
- 5 Step 404 EP2 sends a Call Proceeding message to EP1.
- Step 405 EP2 sends an ARQ message to ZK1.
- Step 406 ZK1 sends either an ACF message or an ARJ message to EP2.
- Step 407 If EP2 receives an ARJ message from ZK1, EP2 sends an Alerting message to EP1.
- 10 Step 408 If EP2 receives an ACF message from ZK1, EP2 sends a Connect message to EP1. The Connect message includes a H.245 control channel port number for use in H. 245 signaling.

ARQ, ACF, and ARJ are messages defined in H.323 for communication between endpoints and Zone Keeper. Set-up, Call Proceeding, Alerting, and Connect are  
 15 messages defined in H.323 for endpoint communications.

FIG. 5 is a possible information flow diagram illustrating the call setup process for establishing communication between a calling endpoint and a called endpoint in different H.323 zones.

- 20 Step 501 Endpoint (EP1') 103-1-2 in Security Zone 101-1 sends an ARQ (Admission Request) message to Zone Keeper (ZK1) 102-1.
- Step 502 ZK1 on behalf of EP1' sends an ARQ message to Zone Keeper (ZK2) 102-2, which registers the called endpoint (EP2') 103-2-3.
- Step 503 ZK2 sends an AFC message including the Q.931 port number of EP2' to ZK1.
- 25 Step 504 ZK1 relays the ACF message from ZK1 to EP1'.
- Step 505 EP1', in response to the supplied ACF message, sends a Set-up message to the Q.931 port of EP2'.
- Step 506 EP2' sends a Call Proceeding message to EP1'.
- Step 507 If EP2' accepts the call, it sends an ARQ message to ZK2.
- 30 Step 508 ZK2 sends an ACF message to EP2'.

Step 509 If EP2' receives an ARJ message from ZK2, EP2' sends a Release Complete message to EP1'.

Step 510 If EP2' receives an ACF message from ZK2, EP2' sends a Connect message to EP1'. The Connect message includes a H.245 control channel port number for use in H.245 signaling.

For further details of H.323 see for example, ITU-T Recommendation H.323 (1998), "Packet Based Multimedia Communications Systems".

This embodiment of the invention uses the so-called Direct-routed Call model for setting up communications. One important characteristic of this model is that it requires minimum message exchanges between H.323 entities. Two advantages are realized by employing this Direct-routed model. One advantage is minimizing message exchanges that directly reduce cost. This is because security comes at the cost of performance degradation and added complexity. Another advantage is that the Zone Keeper is only involved in RAS message exchanges. This improves the scalability of the architecture since the Zone Keeper communication is eliminated as a possible performance bottleneck.

Under the Direct-routed Call model, steps 405 and 406 in FIG. 4, and steps 507 and 508 in FIG5 can be avoided.

FIG. 6 is a diagram illustrating how an embodiment of the invention is implemented under the H.323 framework for securing intra-zone communication. This implementation of this embodiment of the invention assumes the following:

- Zone Keeper is implemented by a H.323 Gatekeeper.
- All users/endpoints are authenticated by ID/Password and a challenge-response protocol. The latter ensures that the password is not sent directly for the authentication purpose. Instead, an endpoint must prove a user's identity by generating a response using his/her password according to a randomly created challenge.

Additionally, the following security tokens, i.e., self-contained security information, are defined here and employed in establishing intra-zone communication between a caller and callee. Under H.235, the security standard for H.323, the so-called cryptoHashedToken is employed, where a message checksum is included in the security

token to ensure its integrity. Particularly, a receiver can detect whether any original information has been tampered with by re-computing its checksum.

- 5           • EPPwdHash – Sent by caller to its Zone Keeper. It contains the information required for authenticating messages sent by a registered caller. To avoid replay attack, where a security intruder copies this information and pretends to be the caller, the following information may be included:

  - time stamp: information concerning when the token is created.
  - a random value to ensure the uniqueness of the hash.
- 10          • ZKIdenSign – Sent by the Zone Keeper to the caller. It contains a signature by the Zone Keeper so that the caller can authenticate the message is indeed from its Zone Keeper. Again, to avoid replay attack, both time stamp and a random value should be included in the creation of the signature. Also included in the token is the response that the caller will use to authenticate the callee.
- 15          • ZKAuthorize – Created by the Zone Keeper and sent to the calling endpoint, which then forwards the token to the callee. This token shall contain information that conveys the authorization and authentication given to the caller by the Zone Keeper. An example of this information includes:

  - Caller's network address
  - 20          – Callee's network address
  - Conference ID
  - Conference goal
  - Valid time interval. The token has to be presented within this time frame to be considered valid.

25           Additionally, this token includes a challenge value for the callee.

- EPHashResp – Created by the callee and returned to the caller. It contains information required for authenticating the callee to the caller. At the minimum, both time stamp and a random value should be included in the creation of the token to avoid replay attack.

30           Referring to FIG. 6, shown are the steps in setting up an intra-zone communication between two endpoints in a Security Zone. In this example, endpoint



(EP1) 103-1-1 and (EP2) 103-1-2 and including Zone Keeper (ZK1) 102-1 in Security Zone 101-1 of FIG. 1. Specifically, the steps taken in setting up the intra-zone communication are as follows:

- 5           1. Endpoint (EP1) 103-1-1 sends an ARQ message, an Admission Request message defined in H.323 for Gatekeeper (Zone Keeper) including an EPPwdHash token, to Zone Keeper (ZK1) 102-1.
2. ZK1 authenticates the EPPwdHash token using a password registered by the user employing EP1.
3. If ZK1 determines that the communication should be allowed, it creates both  
10           ZKIdenSign and ZKAuthorize tokens using its private-key. Then, the ZKIdenSign and ZKAuthorize tokens are inserted into an ACF message, a Request Confirmation message, which is sent to EP1. ACF is a H.323 Zone Keeper (Gatekeeper) message.
4. EP1 authenticates the ZKIdenSign token in the ACF message with the public-  
15           key of ZK1.
5. EP1 extracts the ZKAuthorize token from the ACF message. Then, EP1 sends a Set-up message including the ZKAuthorize token to endpoint (EP2) 103-1-2. The Set-up message is a H.323 message defined for endpoint communication.
- 20           6. EP2 authenticates the ZKAuthorize token in the Set-up message using the public-key of ZK1.
7. EP2 extracts the challenge value included in the ZKAuthorize token and generates a response using its user's password. An EPHashResp token including the response is created.
- 25           8. EP2 sends a H.323 Call Proceeding message including the EPHashResp token to EP1.
9. EP1 authenticates the EPHashResp token to authenticate EP2.

30           Note that in this intra-zone communication scenario, that ZK1 is able to authorize an intra-zone communication. Additionally, both EP1 and EP2 are able to authenticate each other.

FIG. 7 is a diagram illustrating an embodiment of the invention that is implemented under the H.323 framework for securing inter-zone communication. This implementation of an embodiment of the invention also employs the process described above for setting up an intra-zone communication (FIG. 6). Additionally, a new security token is added for inter-zone communication security, namely,

- ZKZKIden – Sent by one Zone Keeper to another. It includes the information needed by the callee to authenticate the caller. An example of this information includes
  - Valid time interval
  - A random value
  - Zone Keeper ID

Referring to FIG. 7, shown are the steps in setting up an inter-zone communication between two endpoints in two different Security Zones. In this example, endpoint (EP1') 103-1-2 in Security Zone (SZ1) 101-1 and including Zone Keeper (ZK1) 102-1, and endpoint (EP2') 103-2-3 in Security Zone (SZ2) 101-2 including Zone Keeper (ZK2) 102-2 of FIG. 1. Specifically, the steps taken in setting up the inter-zone communication are as follows:

1. EP1' sends an ARQ message including the EPPwdHash token of EP1' to ZK1. ZK1 authenticates the EPPwdHash token using EP1's user password. If ZK1 allows the communication, it sends an ARQ message, on behalf of EP1' to ZK2 in SZ2.
  - ZK1 creates a ZKZKIden token using its private-key and includes it in the ARQ message.
  - Determining that the ARQ message is from a different zone than SZ2, ZK2 uses the public-key for ZK1 to authenticate the ZKZKIden token.
2. If ZK2 allows the communication, it creates a ZKAuthorize token using its private-key. This ZKAuthorize token represents ZK2's authorization. Additionally, ZK2 creates a ZKZKIden token for authenticating itself to ZK1. The ZKAuthorize and ZKZKIden tokens are included in an ACF message and, thereby, returned to ZK1.

3. After ZK1 authenticates the ZKZKIden token using ZK2's public-key, ZK1 sends the ACF to EP1'.

- ZK1 creates its own ZKIdenSign token and includes it in the ACF message. The response field in the ZKZKIden token is copied to the ZKIdenSign token.
- ZK1 replaces the ZKZKIden token by its ZKIdenSign token in the ACF. EP1' does not make any modification to the ZKAuthorize token in the ACF message.

4. After authenticating the ZKIdenSign token in the ACF message, EP1' sends a Set-up message including a ZKAuthorize token including a prescribed challenge value to EP2'.

- EP2' authenticates the ZKAuthorize token using ZK2's public-key.
- EP2' extracts a challenge value included in the ZKAuthorize token and generates a response using its user's password. An EPHashResp including the response is created.

5. EP2' sends a Call Proceeding message including the EPHashResp token to EP1'.

- EP1' authenticates responses in both the ZKIdenSign token and the EPHashResp token to authenticate EP2'.

The inter-zone scenario outlined by the above steps shows that both Zone Keepers, ZK1 and ZK2, are able to perform communication access control for inter-zone a communication. Additionally, endpoints, for example, EP1' and EP2', in different zones are able to authenticate each other. It is particularly important that endpoints can authenticate requests from other zones as though they were all in the same zone.

The above described embodiments are, of course, merely illustrative of the principles of the invention. Indeed, numerous other methods or apparatus may be devised by those skilled in the art without departing from the spirit and scope of the invention.

**What is claimed is:**

1           1. A method for establishing a secure communication between users employing  
2 endpoints in a system including one or more security zones, each security zone including  
3 one or more of said endpoints and a Zone Keeper, wherein at least one of said users is a  
4 caller utilizing a first endpoint in one of said one or more security zones and at least  
5 another one of said users is a callee utilizing a second endpoint in one of said one or more  
6 security zones, the method including the steps of:

7           said caller sending a communication request message including a communication  
8 request for establishing a secure multimedia communication including security  
9 information identifying said caller, via said first endpoint to a first one of said Zone  
10 Keepers associated with a security zone including said first endpoint;

11           said first Zone Keeper authenticating the identity of said caller, and if said caller  
12 identity is authenticated, authorizing said caller's communication request;

13           said first Zone keeper determining whether said requested secure communication  
14 is an intra-zone or an inter-zone communication:

15           if said requested communication is an intra-zone communication both said first  
16 and second endpoints are in the same security zone, said first Zone Keeper in conjunction  
17 with said first and second endpoints in said first security zone establishing said secure  
18 communication between said caller and said callee;

19           if said requested communication is an inter-zone communication said first and  
20 second endpoints are in first and second security zones, respectively, said first Zone  
21 Keeper sending said request message to said second Zone Keeper associated with said  
22 second security zone; and

23           establishing said secure inter-zone communication utilizing said first Zone  
24 Keeper, said first endpoint in said first security zone, said second Zone Keeper and said  
25 second endpoint in said second security zone.

1           2. The method as defined in claim 1 further including providing a capability by  
2 each of said Zone Keepers for users of an endpoint in a security zone associated with a  
3 particular Zone Keeper to register authentication keys and/or methods and said particular  
4 Zone Keeper authenticating said users only through said registered keys and/or methods  
5 to honor requests for secure communication.

1           3. The method as defined in claim 1 further including providing a capability by  
2 each of said Zone Keepers to have registered authentication keys and/or methods of  
3 endpoints in a security zone associated with a particular Zone Keeper and said particular  
4 Zone Keeper authenticating only users authenticated by said user authentication keys  
5 and/or methods and said endpoint authentication keys and/or methods to honor requests  
6 for secure communication.

1           4. The invention as defined in claim 1 further including providing a capability by  
2 each of said Zone Keepers to have registered by users using an endpoint associated with a  
3 particular Zone Keeper individual prescribed security policies and said particular Zone  
4 Keeper enforcing said prescribed security policies.

1           5. The method as defined in claim 1 wherein said intra-zone communication is  
2 established by the further steps of

3           said first Zone Keeper sending an authorization message including an  
4 authorization of said caller communication request to said caller, via said first endpoint,  
5 said authorization including security information identifying said first Zone Keeper and  
6 security information identifying said callee;

7           said caller authenticating the authorization sent by said first Zone Keeper;

8           said caller sending, via said first endpoint, a connection request message  
9 including a communication proposal for establishing a multimedia communication  
10 connection with said callee, via said second endpoint;

11          said callee authenticating said authorization and said communication proposal;

12          said callee sending, via said second endpoint, to said caller via said first endpoint,  
13 an acceptance message indicating that said callee accepts the communication proposal,  
14 said message including security information identifying said callee;

15          said caller authenticating the identity of said callee; and

16          if said caller authenticates said identity of said callee, establishing said caller and  
17 said callee communication through said first and second endpoints in said first security  
18 zone, wherein a secure multimedia communication is established.

1           6. The method as defined in claim 5 further including, if said first Zone Keeper  
2 rejects said communication request from said caller, said first Zone Keeper sending an

3 authorization rejected message indicating that said communication request was rejected  
4 to said caller, via said first endpoint.

1 7. The method as defined in claim 5 wherein said connection request message  
2 includes said communication authorization and security information for authenticating  
3 the identity of said callee.

1 8. The method as defined in claim 7 wherein said connection message further  
2 includes a proposal indicating how the caller-callee communication should be set-up.

1 9. The method as defined in claim 5 further including said first Zone Keeper  
2 employing a prescribed security arrangement for authenticating the identity of said caller.

1 10. The method as defined in claim 9 wherein said prescribed security  
2 arrangement includes using a caller identification (ID) and corresponding password.

1 11. The method as defined in claim 5 wherein said connection request message  
2 includes said authorization from said Zone Keeper, security information identifying said  
3 caller to said callee and a communication proposal of how the secure caller - callee  
4 communication connection is to be set-up.

1 12. The method as defined in claim 11 wherein said connection request message  
2 further includes security information for authenticating the identity of said callee.

1 13. The invention as defined in claim 11 further including said first Zone Keeper  
2 providing authentication of its identity by using public-key cryptography and a digital  
3 signature and wherein said users authenticate the first Zone Keeper identity by employing  
4 said first Zone Keeper's public key.

1 14. The invention as defined in claim 13 further obtaining said digital signature  
2 by said first Zone Keeper signing said request response message with a private-key.

1 15. The method as defined in claim 1 wherein said inter-zone communication is  
2 established by the further steps of

3 said first Zone Keeper forwarding said communication request message to a  
4 second Zone Keeper associated with said second security zone;

5 said second Zone Keeper authenticating that the communication request message  
6 is from said first Zone Keeper;

7 said second Zone Keeper sending an authorization message including an  
8 authorization of said caller communication request to said first Zone Keeper, said

9 authorization message including security information identifying said second Zone  
10 Keeper and security information identifying said callee;  
11 said first Zone Keeper authenticating the authorization in said authorization  
12 message sent by said second Zone Keeper;  
13 if said authorization in said authorization message is authenticated, said first Zone  
14 keeper sending said authorization message to said caller via said first endpoint;  
15 said caller sending, via said first endpoint, a connection request message  
16 including a communication proposal for establishing a secure multimedia communication  
17 connection with said callee, via said second endpoint;  
18 said callee authenticating said authorization and said communication proposal;  
19 said callee sending, via said second endpoint, to said caller via said first endpoint,  
20 an acceptance message indicating that callee accepts the communication proposal, said  
21 message including security information identifying said callee;  
22 said caller authenticating the identity of said callee; and  
23 if said caller authenticates said identity of said callee, establishing said caller and  
24 said callee communication through said first and second endpoints, wherein a secure  
25 multimedia communication is established.

1 16. The method as defined in claim 15 further including, if said first Zone Keeper  
2 rejects said communication request from said caller, said first Zone Keeper sending an  
3 authorization rejected message indicating that said communication request was rejected  
4 to said caller, via said first endpoint.

1 17. The method as defined in claim 15 further including said first Zone Keeper  
2 determining whether said caller and said callee are security compatible for the requested  
3 secure multimedia communication.

1 18. The method as defined in claim 17 wherein each of said Zone Keepers has its  
2 own private key, and further including said first Zone Keeper signing said  
3 communication request message and said second Zone Keeper authenticating that said  
4 communication request message was sent by said first Zone Keeper through said first  
5 Zone Keeper's private key.

1 19. The method as defined in claim 18 wherein each of said Zone Keepers has its  
2 own digital signature, and further including security information indicating the identity of

3 said callee and said second Zone Keeper including its digital signature in said  
4 authorization message sent to said first Zone Keeper, and said first Zone Keeper  
5 authenticating the authorization sent by said second Zone Keeper through the digital  
6 signature of said second Zone Keeper.

1 20. The method as defined in claim 19 wherein each of said Zone keepers has its  
2 own public key, said caller authenticates said authorization by verifying said digital  
3 signature of said first Zone Keeper and said callee authenticates said authorization and  
4 communication proposal by verifying the digital signature of said second Zone Keeper  
5 through its public key.

1 21. The method as defined in claim 1 wherein each of said users has its own  
2 password which is registered by the user of an endpoint with the endpoint's associated  
3 Zone Keeper, and each of said Zone Keepers has its own private key and its own public  
4 key and further including said communication request message including a first  
5 prescribed security token, said first Zone Keeper authenticating said first prescribed  
6 security token, and if said first prescribed security token is authenticated, determining  
7 that said communication should be allowed.

1 22. The method as defined in claim 21 wherein said intra-zone communication is  
2 established by the further steps of

3 said first Zone Keeper generating a second prescribed security token and a third  
4 prescribed security token, inserting said second and third prescribed security tokens in an  
5 authentication message and sending said authorization message to said first endpoint, said  
6 third prescribed security token including a prescribed challenge value;

7 said first endpoint authenticating said second prescribed security token in said  
8 authorization message and extracting said third prescribed security token;

9 said first endpoint sending a communication set-up message including said third  
10 prescribed security token to said second endpoint;

11 said second endpoint authenticating said third prescribed security token in said  
12 set-up message;

13 said second endpoint extracting said challenge value from said third prescribed  
14 security token and generating a response;

15 generating a fourth prescribed security token including said response;



16           said second endpoint sending a call proceeding message including said fourth  
17 prescribed security token to said first endpoint;

18           said first endpoint authenticating said fourth prescribed security token to  
19 authenticate said second endpoint; and

20           if said second endpoint is authenticated, establishing said secure multimedia  
21 communication using said first and second endpoints.

1           23. The method as defined in claim 22 wherein said first prescribed security  
2 token is authenticated by employing the password registered by said user of said first  
3 endpoint.

1           24. The method as defined in claim 23 wherein said second and third prescribed  
2 security tokens are generated using said Zone Keeper's private-key.

1           25. The method as defined in claim 24 wherein said second prescribed security  
2 token is authenticated by said first endpoint using said Zone Keeper's public-key.

1           26. The method as defined in claim 25 wherein said third prescribed security  
2 token is authenticated by said second endpoint using said Zone Keeper's public-key.

1           27. The method as defined in claim 26 wherein said response is generated using  
2 said registered password of said user of said second endpoint.

1           28. The method as defined in claim 27 wherein said first prescribed security  
2 token is an EPPwdHash security token, said second prescribed security token is a  
3 ZKIdenSign security token, said third prescribed security token is a ZKAuthorize security  
4 token and said fourth prescribed security token is an EPHashResp security token.

1           29. The method as defined in claim 21 wherein said inter-zone communication is  
2 established by the further steps of

3           said first Zone Keeper generating a second prescribed security token and  
4 including it in a second communication request message;

5           said first Zone Keeper sending said second communication request message to  
6 said second Zone keeper;

7           said second Zone Keeper determining that said second communication request  
8 message from a different security zone than the security zone including said second Zone  
9 Keeper, authenticates said second prescribed security token;

10 if said second Zone Keeper authorizes said communication request in said second  
11 communication request message, said second Zone Keeper generating a third prescribed  
12 security token and a fourth prescribed security token;

13 said second Zone Keeper generating a second communication authorization  
14 message including said third and fourth prescribed security tokens and sending said  
15 second communication authorization message to said first Zone Keeper;

16 said first Zone Keeper authenticating said fourth prescribed security token and if  
17 authenticated generating a fifth prescribed security token and replaces it for said fourth  
18 prescribed security token in said second communication authorization message to  
19 generate a modified second authorization communication message, and sending said  
20 modified second authorization communication message to said first endpoint;

21 said first endpoint authenticating said fifth prescribed security token in said  
22 modified second communication request message;

23 if said fifth prescribed security token is authenticated, said first endpoint  
24 generating a communication set-up message including a sixth prescribed security token  
25 including a prescribed challenge value and sending said communication set-up message  
26 to said second endpoint;

27 said second endpoint authenticating said sixth prescribed security token,  
28 extracting said prescribed challenge value and generating a response;

29 generating a seventh prescribed security token including said response;

30 said second endpoint generating and sending a call proceeding message including  
31 said seventh prescribed security token to said first endpoint;

32 said first endpoint authenticating said responses in said fifth and seventh  
33 prescribed security tokens to authenticate said second endpoint; and

34 if said second endpoint is authenticated, establishing said secure multimedia  
35 communication using said first and second endpoints.

1 30. The method as defined in claim 29 wherein said first prescribed security  
2 token is authenticated by employing the password registered by said user of said first  
3 endpoint.

1 31. The method as defined in claim 30 wherein said second prescribed security  
2 token is generated using said first Zone Keeper's private-key.

1           32. The method as defined in claim 31 wherein said second prescribed security  
2 token is authenticated by said second Zone Keeper using said first Zone Keeper's public-  
3 key.

1           33. The method as defined in claim 32 wherein said third prescribed security  
2 token is generated by said second Zone Keeper using said second Zone Keeper's private-  
3 key.

1           34. The method as defined in claim 33 wherein said fourth prescribed security  
2 token is generated by said second Zone Keeper using said second Zone Keeper's private-  
3 key.

1           35. The method as defined in claim 34 wherein said first Zone Keeper  
2 authenticates said fourth prescribed security token using said second Zone Keeper's  
3 public-key.

1           36. The method as defined in claim 35 wherein said first Zone Keeper generates  
2 said fifth prescribed security token using said first Zone Keeper's private-key.

1           37. The method as defined as defined in claim 36 wherein said fifth prescribed  
2 security token is authenticated by said first endpoint using said first Zone Keeper's  
3 public-key.

1           38. The method as defined in claim 37 wherein said sixth prescribed security  
2 token is authenticated by said second endpoint using said second Zone Keeper's public-  
3 key.

1           39. The method as defined in claim 38 wherein said response is generated using  
2 said registered password of said user of said second endpoint.

1           40. The method as defined in claim 39 wherein said first prescribed security  
2 token is an EPPwdHash security token, said second prescribed security token is a  
3 ZKZKIden security token, said third prescribed security token is a ZKAuthorize security  
4 token, said fourth prescribed security token is a second ZKZKIden security token, said  
5 fifth prescribed security token is a ZKIdenSign security token, said sixth prescribed  
6 security token is a second ZKAuthorize security token and said seventh prescribed  
7 security token is an EPHashResp security token.

8           41. A method for establishing a secure communication between users employing  
9 endpoints in a security zone including a plurality of said endpoints and a Zone Keeper,

10 wherein at least one of said users is a caller utilizing an associated one of said endpoints  
11 in said security zone and at least another one of said users is a callee utilizing an  
12 associated another of said endpoints in said security zone, the method including the steps  
13 of:

14       said at least one caller sending a communication request message including a  
15 communication request for establishing a multimedia communication including security  
16 information identifying said caller, via said associated one of said endpoints to said Zone  
17 Keeper;

18       said Zone Keeper authenticating the identity of said caller, and if said caller  
19 identity is authenticated, authorizing said caller's communication request;

20       said Zone Keeper sending an authorization message including an authorization of  
21 said caller communication request to said caller, via said associated one of said  
22 endpoints, said authorization including security information identifying said Zone Keeper  
23 and security information identifying said callee;

24       said caller authenticating the authorization sent by said Zone Keeper;

25       said caller sending, via said associated one of said endpoints, a connection request  
26 message including a communication proposal for establishing a multimedia  
27 communication connection with said callee, via said associated another of said endpoints;

28       said callee authenticating said authorization and said communication proposal;

29       said callee sending, via said associated another of said endpoints, to said caller  
30 via said associated one of said endpoints, an acceptance message indicating that callee  
31 accepts the communication proposal, said message including security information  
32 identifying said callee;

33       said caller authenticating the identity of said callee; and

34       if said caller authenticates said identity of said callee, establishing said caller and  
35 said callee communication through said associated one of said endpoints and said  
36 associated another of said endpoints, wherein a secure multimedia communication is  
37 established.

1       42. The method as defined in claim 41 further including, if said Zone Keeper  
2 rejects said communication request from said caller, said Zone Keeper sending an

3 authorization rejected message indicating that said communication request was rejected  
4 to said caller, via said associated one of said endpoints.

1 43. The method as defined in claim 41 wherein said connection request message  
2 includes said communication authorization and security information for authenticating  
3 the identity of said callee.

1 44. The method as defined in claim 43 wherein said connection message further  
2 includes a proposal indicating how the caller-callee communication should be set-up.

1 45. The method as defined in claim 41 further including said Zone Keeper  
2 employing a prescribed security arrangement for authenticating the identity of said caller.

1 46. The method as defined in claim 45 wherein said prescribed security  
2 arrangement includes using a caller identification (ID) and corresponding password.

1 47. The method as defined in claim 41 wherein said connection request message  
2 includes said authorization from said Zone Keeper, security information identifying said  
3 caller to said callee and a communication proposal of how the secure caller – callee  
4 communication connection is to be set-up.

1 48. The method as defined in claim 47 wherein said connection request message  
2 further includes security information for authenticating the identity of said callee.

1 49. The method as defined in claim 48 further including providing a capability  
2 by said Zone Keeper for users of an endpoint in said security zone to register  
3 authentication keys and/or methods and said Zone Keeper authenticating said users only  
4 through said registered keys and/or methods to honor requests for secure communication.

1 50. The method as defined in claim 49 further including providing a capability by  
2 said Zone Keeper to have registered authentication keys and/or methods of endpoints in  
3 said security zone and said Zone Keeper authenticating only users authenticated by said  
4 user authentication keys and/or methods and said endpoint authentication keys and/or  
5 methods to honor requests for secure communication.

1 51. The invention as defined in claim 47 further including providing a capability  
2 by said Zone Keeper to have registered by users individual prescribed security policies  
3 and said Zone Keeper enforcing said prescribed security policies.

1           52. The invention as defined in claim 47 further including said Zone Keeper  
2 providing authentication of its identity by using public-key cryptography and a digital  
3 signature and wherein said users authenticate the Zone Keeper identity by employing said  
4 Zone Keeper's public key.

1           53. The invention as defined in claim 52 further obtaining said digital signature  
2 by said Zone Keeper signing said request response message with a private-key.

1           54. A method for establishing a secure communication between users employing  
2 endpoints in a system including one or more security zones, each security zone including  
3 one or more of said endpoints and a Zone Keeper, wherein at least one of said users is a  
4 caller utilizing a first endpoint in one of said one or more security zones and at least  
5 another one of said users is a callee utilizing a second endpoint in one of said one or more  
6 security zones, the method including the steps of:

7           said caller sending a communication request message including a communication  
8 request for establishing a secure multimedia communication including security  
9 information identifying said caller, via said first endpoint to a first one of said Zone  
10 Keepers associated with a security zone including said first endpoint;

11           said first Zone Keeper authenticating the identity of said caller, and if said caller  
12 identity is authenticated, authorizing said caller's communication request;

13           said first Zone keeper determining whether said endpoint being used by said  
14 callee is in said first security zone or in a second one of said security zones;

15           if it is determined that said second endpoint in said second security, said first  
16 Zone Keeper forwarding said communication request message to a second Zone Keeper  
17 associated with said second security zone;

18           said second Zone Keeper authenticating that the communication request message  
19 is from said first Zone Keeper;

20           said second Zone Keeper sending an authorization message including an  
21 authorization of said caller communication request to said first Zone Keeper, said  
22 authorization message including security information identifying said second Zone  
23 Keeper and security information identifying said callee;

24           said first Zone Keeper authenticating the authorization in said authorization  
25 message sent by said second Zone Keeper;

26 if said authorization in said authorization message is authenticated, said first Zone  
27 keeper sending said authorization message to said caller via said first endpoint;  
28 said caller sending, via said associated one of said endpoints, a connection request  
29 message including a communication proposal for establishing a secure multimedia  
30 communication connection with said callee, via said second endpoint;  
31 said callee authenticating said authorization and said communication proposal;  
32 said callee sending, via said second endpoint, to said caller via said first endpoint,  
33 an acceptance message indicating that callee accepts the communication proposal, said  
34 message including security information identifying said callee;  
35 said caller authenticating the identity of said callee; and  
36 if said caller authenticates said identity of said callee, establishing said caller and  
37 said callee communication through said first and second endpoints, wherein a secure  
38 multimedia communication is established.

1 55. The method as defined in claim 54 further including, if said first Zone Keeper  
2 rejects said communication request from said caller, said first Zone Keeper sending an  
3 authorization rejected message indicating that said communication request was rejected  
4 to said caller, via said first endpoint.

1 56. The method as defined in claim 54 further including said first Zone Keeper  
2 determining whether said caller and said callee are security compatible for the requested  
3 secure multimedia communication.

1 57. The method as defined in claim 56 wherein each of said Zone Keepers has its  
2 own private key, and further including said first Zone Keeper signing said  
3 communication request message and said second Zone Keeper authenticating that said  
4 communication request message was sent by said first Zone Keeper through said first  
5 Zone Keeper's private key.

1 58. The method as defined in claim 57 wherein each of said Zone Keepers has its  
2 own digital signature, and further including security information indicating the identity of  
3 said callee and said second Zone Keeper including its digital signature in said  
4 authorization message sent to said first Zone Keeper, and said first Zone Keeper  
5 authenticating the authorization sent by said second Zone Keeper through the digital  
6 signature of said second Zone Keeper.

- 1           59. The method as defined in claim 58 wherein each of said Zone keepers has its
- 2     own public key, said caller authenticates said authorization by verifying said digital
- 3     signature of said first Zone Keeper and said callee authenticates said authorization and
- 4     communication proposal by verifying the digital signature of said second Zone Keeper
- 5     through its public key.



**Abstract of the Disclosure**

A two-tier security architecture that provides balance between the use of public and secret-key cryptography to realize cost-effectiveness and scalability of security. One tier is an intra-zone tier and the other tier is an inter-zone tier. The intra-zone tier addresses communication between users employing endpoints within a prescribed Security Zone and is designed to achieve cost-effectiveness. The inter-zone tier specifies how communication between users employing endpoints from different Security Zones can be established and is designed to provide scalability for intra-enterprise and/or inter-enterprise communications. Specifically, each Security Zone has a "Zone Keeper" and one or more endpoints that may be employed by users. The Zone Keeper authenticates, i.e., validates, users employing an endpoint in the Security Zone and determines whether a caller and a callee are security compatible. When setting up a communication, the caller provides the Zone Keeper security information in order for the caller to prove its identity. The callee supplies to the caller information confirming its identity. A proposal on how the communication is to be Set-up is sent from the caller to the callee, and if they agree to the proposal and their security is authenticated, the communication is started. For inter-zone, inter-domain, communications, the caller provides information as described above to its Zone Keeper. Then, the caller's Zone Keeper forwards the caller's request to the Zone Keeper of the security associated with the callee. Additionally, the caller's Zone Keeper also supplies the callee's Zone Keeper with its security identity so that the callee's Zone Keeper may authenticate that the request is from the caller's Zone Keeper. Then, the callee's Zone Keeper sends back an authorization to the Caller's Zone Keeper. This authorization includes the callee's Zone Keeper security identity so that the caller's Zone Keeper can authenticate that the authorization is from the callee's Zone Keeper. Then, as indicated above, the callee supplies to the caller information confirming its identity. A proposal on how the communication is to be Set-up is sent from the caller to the callee and if they agree to the proposal, and their security is authenticated, the communication is started.

FIG. 1

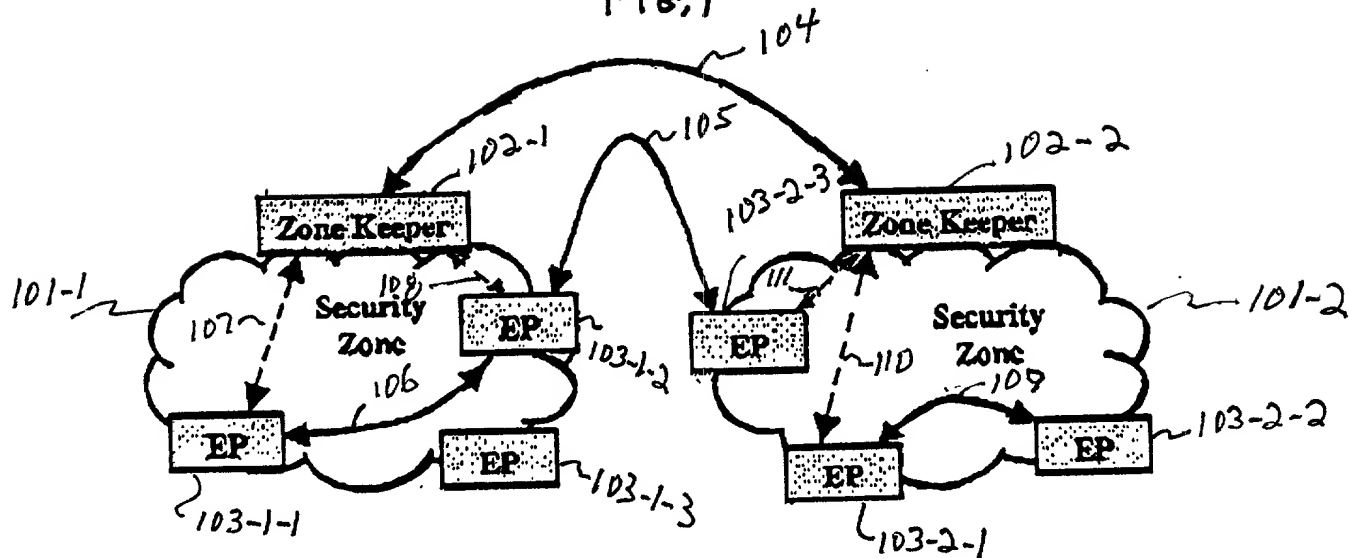


FIG. 2

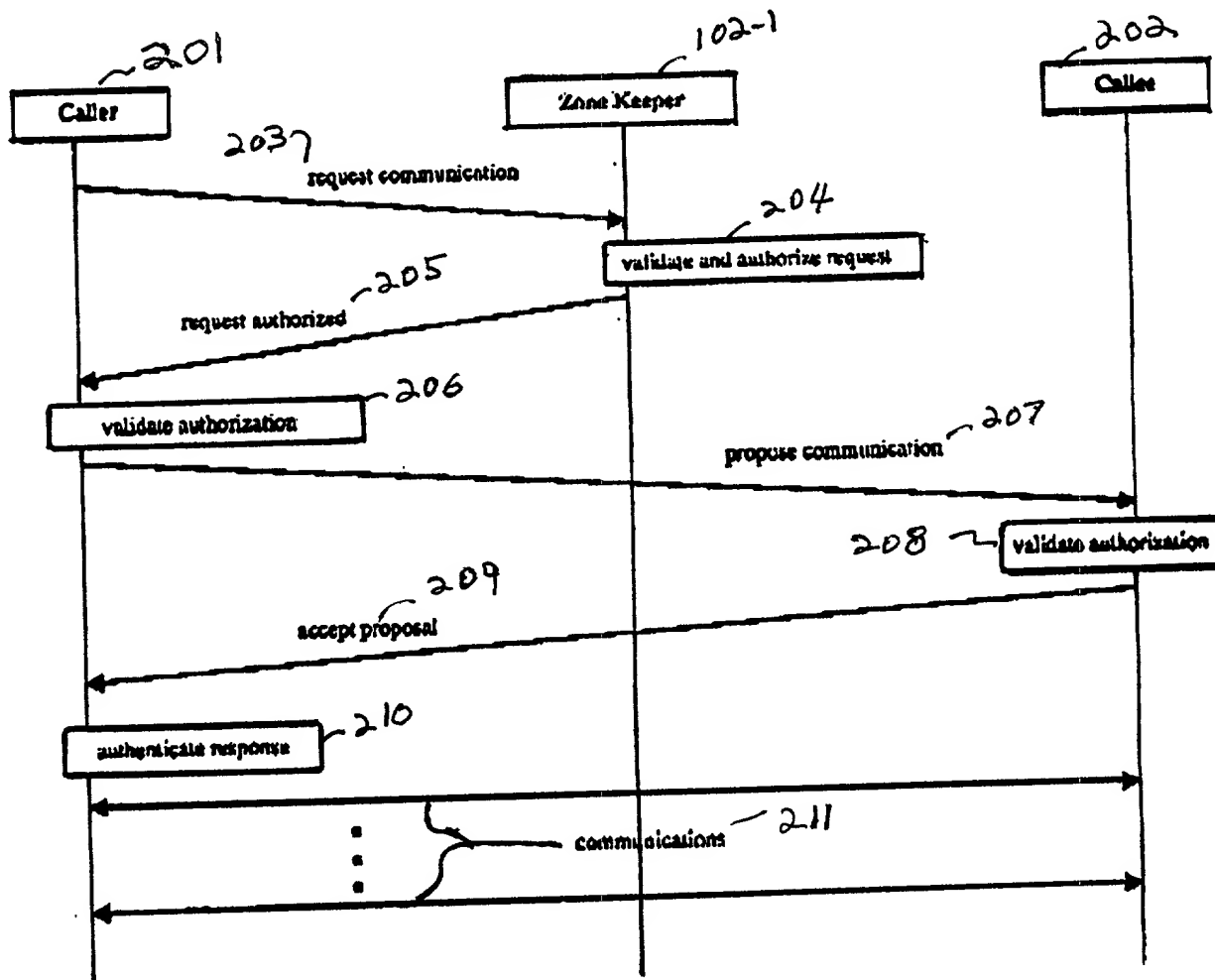
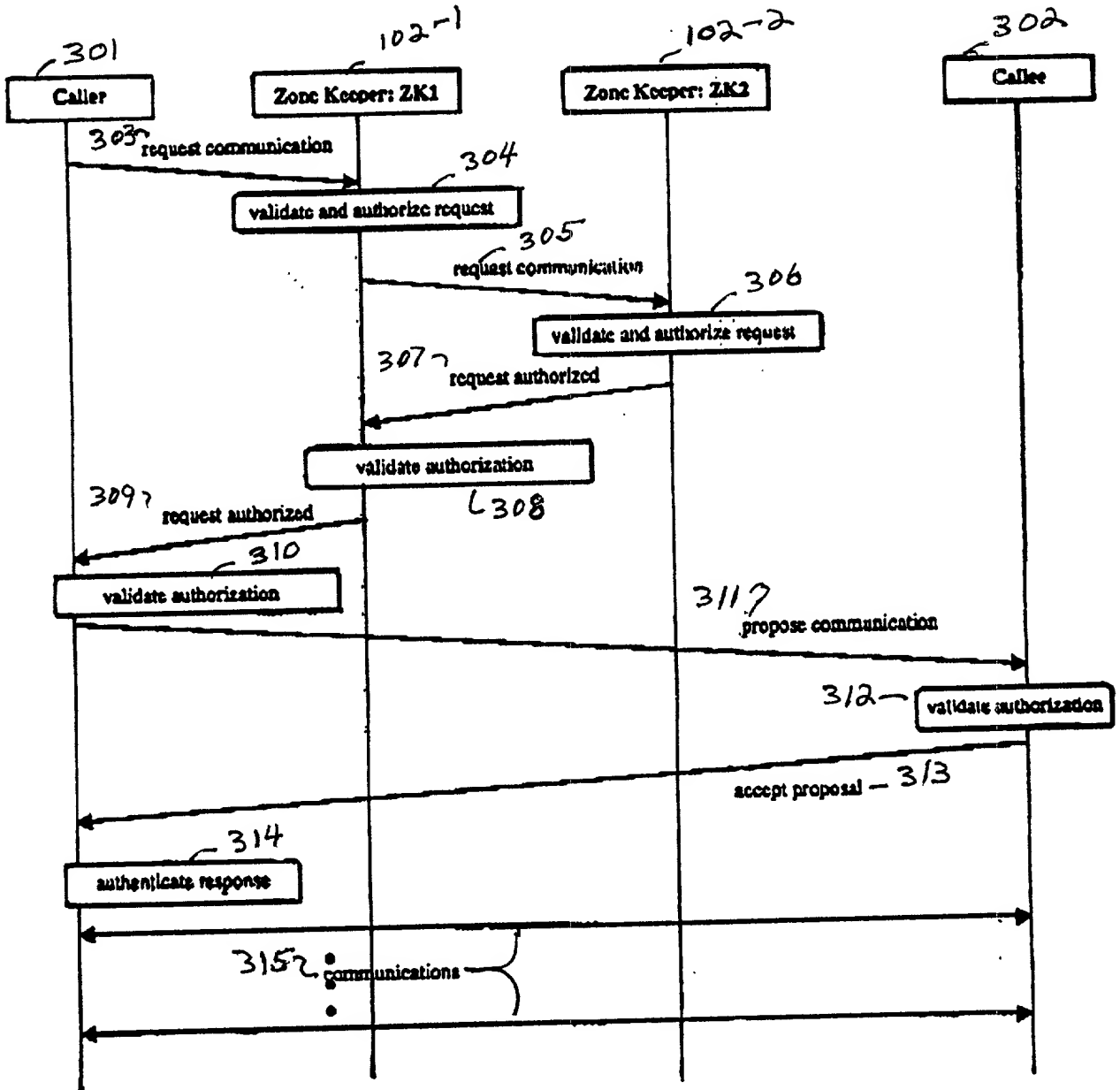


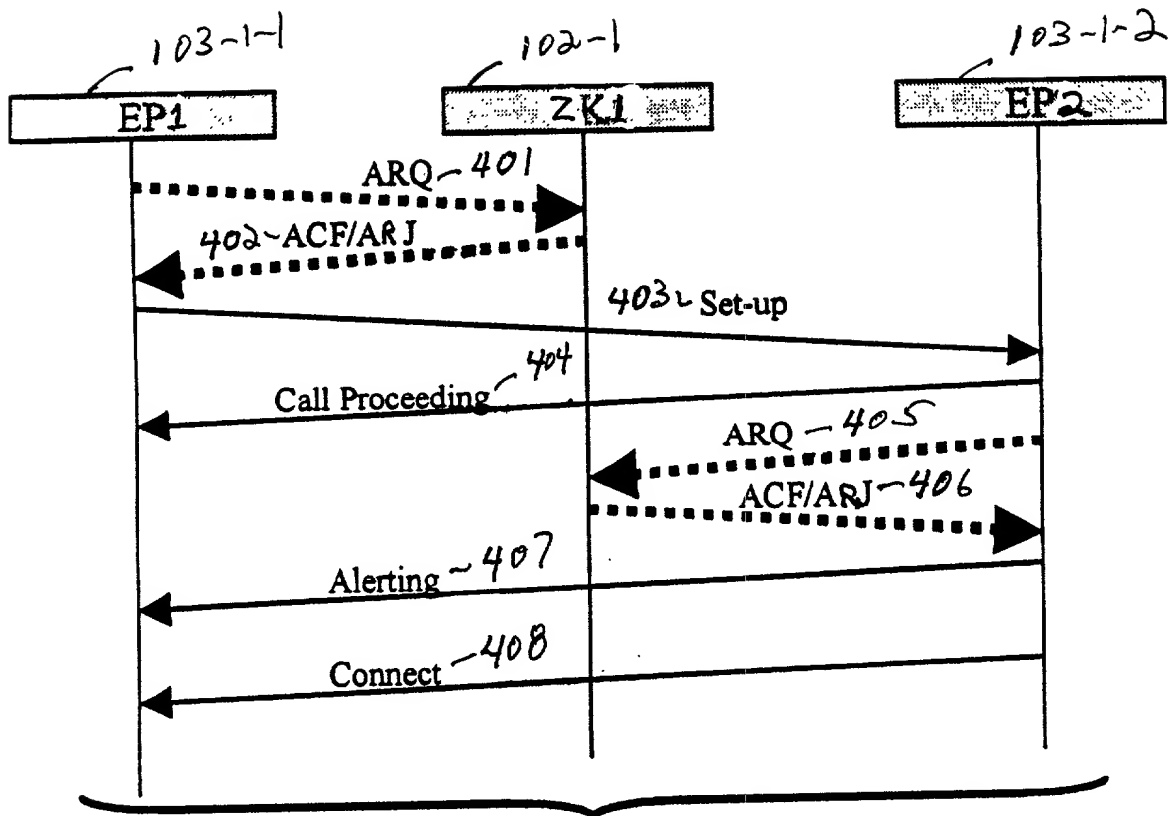
FIG. 3



Y. HSU 1

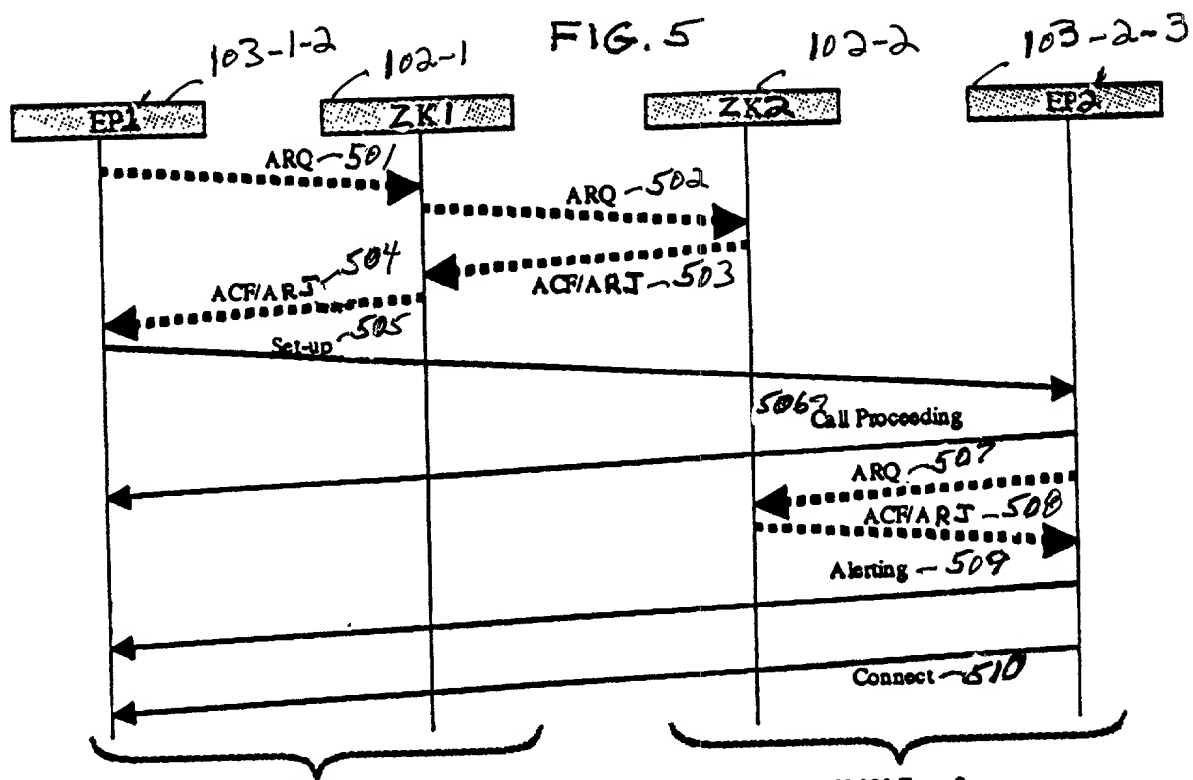
3/5

FIG. 4



H.323 Zone

FIG. 5



H.323 Zone 1

H.323 Zone 2

FIG. 6

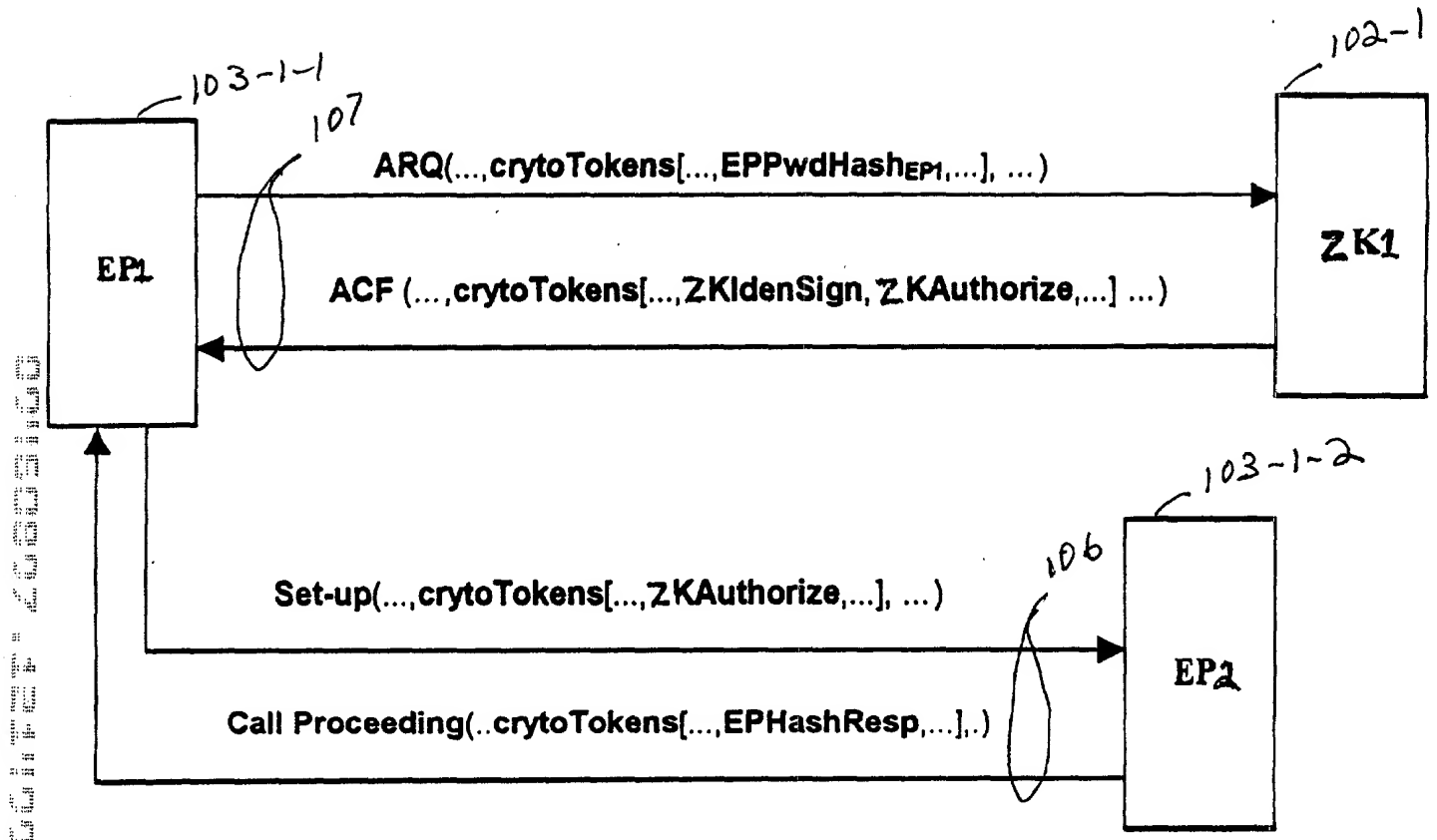
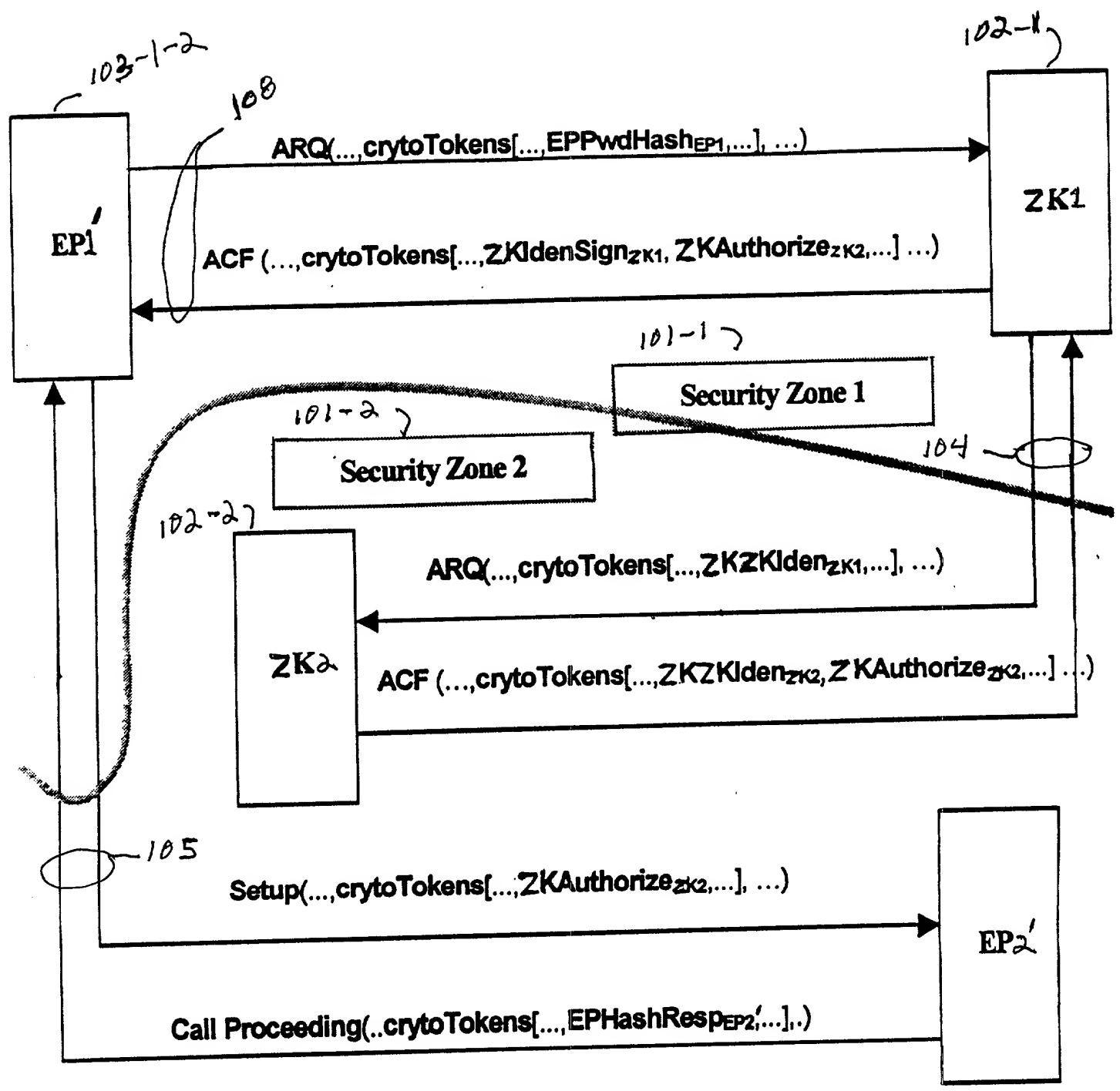


FIG. 7



, IN THE UNITED STATES  
PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney

As the below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **DUAL-TIER SECURITY ARCHITECTURE FOR INTER-DOMAIN ENVIRONMENTS** the specification of which is attached hereto and which was filed as a Provisional Application Serial No. 60/129486 on April 15, 1999.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to in this oath or declaration.

I acknowledge the duty to disclose all information known to me which is material to patentability as defined in Title 37, Code of Federal Regulations, 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

None

I hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

None

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Lester H. Birnbaum	(Reg. No. 25830)
Richard J. Botos	(Reg. No. 32016)
Jeffery J. Brosemer	(Reg. No. 36096)
Kenneth M. Brown	(Reg. No. 37590)
Craig J. Cox	(Reg. No. 39643)
Donald P. Dinella	(Reg. No. 39961)
Guy Eriksen	(Reg. No. 41736)
Martin I. Finston	(Reg. No. 31613)
James H. Fox	(Reg. No. 29379)
William S. Francos	(Reg. No. 38456)
Barry H. Freedman	(Reg. No. 26166)
Julio A. Garceran	(Reg. No. 37138)
Mony R. Ghose	(Reg. No. 38159)
Jimmy Goo	(Reg. No. 36528)
Anthony Grillo	(Reg. No. 36535)
Stephen M. Gurey	(Reg. No. 27336)
John M. Harman	(Reg. No. 38173)
Michael B. Johannesen	(Reg. No. 35557)
Mark A. Kurisko	(Reg. No. 38944)
Irena Lager	(Reg. No. 39260)
Christopher N. Malvone	(Reg. No. 34866)
Scott W. McLellan	(Reg. No. 30776)
Martin G. Meder	(Reg. No. 34674)
John C. Moran	(Reg. No. 30782)
Michael A. Morra	(Reg. No. 28975)
Gregory J. Murgia	(Reg. No. 41209)
Claude R. Narcisse	(Reg. No. 38979)
Joseph J. Opalach	(Reg. No. 36229)
Neil R. Ormos	(Reg. No. 35309)
Eugen E. Pacher	(Reg. No. 29964)
Jack R. Penrod	(Reg. No. 31864)
Daniel J. Piotrowski	(Reg. No. 42079)
Gregory C. Ranieri	(Reg. No. 29695)
Scott J. Rittman	(Reg. No. 39010)
Eugene J. Rosenthal	(Reg. No. 36658)
Bruce S. Schneider	(Reg. No. 27949)
Ronald D. Slusky	(Reg. No. 26585)
David L. Smith	(Reg. No. 30592)
Patricia A. Verlangieri	(Reg. No. 42201)
John P. Veschi	(Reg. No. 39058)
David Volejnicek	(Reg. No. 29355)
Charles L. Warren	(Reg. No. 27407)
Jeffrey M. Weinick	(Reg. No. 36304)
Eli Weiss	(Reg. No. 17765)



I hereby appoint the attorney(s) on ATTACHMENT A as associate attorney(s) in the aforementioned application, with full power solely to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected with the prosecution of said application. No other powers are granted to such associate attorney(s) and such associate attorney(s) are specifically denied any power of substitution or revocation.

Full name of inventor: Yung-Kao Hsu

Inventor's  
signature



Date 12/10/99

Residence: Marlboro, Monmouth County, New Jersey

Citizenship: Republic of China

Post Office Address: 90 Ottawa Road South  
Marlboro, New Jersey 07746

**ATTACHMENT A**

Attorney Name(s): Thomas Stafford Reg No.: 24767  
\_\_\_\_\_  
\_\_\_\_\_

Telephone calls should be made to Thomas Stafford, Patent Attorney at:

Phone No.: 727-772-4173

Fax No.: 727-772-2545

All written communications are to be addressed to:

THOMAS STAFFORD

PATENT ATTORNEY

4173 Rotherham Court

Palm Harbor, Florida 34685